Town of Gardiner

CYBERSECURITY INCIDENT NOTIFICATION GUIDE

Municipal Government Edition

Managed by: MCS Tech Services, LLC

EMERGENCY CONTACT INFORMATION

24/7 Emergency Line: (845) 259-1700
Security Operations Manager: Kevin Cleary
Direct Email: kevin@mcstechinc.com
General Operations Manager: Joshua Moon
Direct Email: joshua@mcstechinc.com
Support Email (Non-Emergency): support@mcstechinc.com
Standard Response Time: 4 hours - 9am-5pm, Monday to Friday
Emergency Response Time: 1 hour (24/7)

1. PURPOSE OF THIS GUIDE

This guide provides clear procedures for town employees and officials to recognize, report, and respond to cybersecurity incidents. Quick and proper reporting is essential to protect town systems, resident data, and ensure compliance with New York State regulations including FOIL, data breach notification requirements, and public records laws.

Time is critical: The faster we know about an incident, the faster we can contain it and minimize impact.

2. WHAT IS A CYBERSECURITY INCIDENT?

A cybersecurity incident is any event that threatens or compromises town systems, data, or operations. If you see something suspicious, report it immediately.

Examples of Incidents You Should Report:

- **Ransomware or System Lockout:** Files are encrypted, systems display ransom messages, or you cannot access your computer
- **Suspicious Emails (Phishing):** Emails asking for passwords, urgent wire transfers, or containing suspicious links/attachments
- **Compromised Credentials:** You accidentally gave your password to someone, clicked a phishing link, or suspect your account was accessed by someone else
- **Malware or Virus Detection:** Antivirus alerts, computer running very slowly, unexpected pop-ups, programs you didn't install
- **Unauthorized Access:** Someone accessed systems they shouldn't have, unknown login attempts, unauthorized accounts discovered
- **Lost or Stolen Devices:** Town laptop, tablet, phone, or USB drive containing town data is missing or stolen
- **Data Breach:** Resident data, confidential town information, or employee data was accessed or disclosed without authorization
- **System Outage or Disruption:** Critical systems down unexpectedly, network not working, email not functioning
- **Unusual System Behavior:** Files disappearing, unexpected password changes, systems behaving strangely
- **Physical Security Breach:** Unauthorized person accessed server room or secured areas containing IT equipment

3. INCIDENT SEVERITY LEVELS

Not all incidents are the same. Understanding severity helps you know how urgently to report.

CRITICAL - CALL IMMEDIATELY	Response: Within 1 Hour (24/7)

- **Active ransomware attack - systems are being encrypted**
- **Widespread system outage affecting town operations**
- **Confirmed data breach involving resident PII (Social Security numbers, financial data)**
- **Critical systems compromised (financial systems, emergency services)**
- **Any incident threatening public safety**
- **Town network completely down or under active attack**

ACTION: CALL (845) 259-1700 IMMEDIATELY - Do not wait, do not email first.

HIGH - CALL WITHIN 1 HOUR	Response: Within 1 Hour

- **Confirmed malware on town systems**
- **Lost/stolen device with unencrypted town or resident data**
- **Successful phishing attack - credentials were entered**
- **Unauthorized access to confidential information**
- **Department systems not functioning**
- **Discovery of unauthorized user accounts**

ACTION: CALL (845) 259-1700 or Email Security Operations Manager within 1 hour.

MEDIUM - REPORT WITHIN 4 HOURS	Response: Within 4 Hours

- **Suspicious emails that were not clicked**
- **Lost/stolen device with encrypted data**
- **Minor system issues or unusual behavior**
- **Policy violations creating potential security risks**
- **Suspicious activity requiring investigation**

ACTION: Email support@mcstechinc.com or call during business hours.

4. WHO SHOULD REPORT INCIDENTS?

EVERYONE has a responsibility to report security incidents. You do not need to be certain something is an incident - if you suspect something is wrong, report it.

Department-Level Responsibilities:

- **All Employees:** Report any suspicious activity immediately. You are the front line of defense.
- **Department Heads:** Ensure incidents affecting your department are reported promptly. Coordinate with IT for department response.
- **Town Clerk:** Report incidents involving public records, FOIL requests, or records management systems.
- **Town Supervisor:** Briefed on all critical incidents. Final authority on external communications and Town Board notification.
- **IT Contact (if designated):** First point of contact within the town. Report to MCS TECH immediately upon discovery.

IMPORTANT: Do not assume someone else will report it. If you see something suspicious, report it yourself.

5. WHAT INFORMATION TO PROVIDE

When reporting an incident, provide as much of the following information as possible:

- What happened? (Describe what you observed) • When did it happen or when did you discover it?
- What system or device is affected? (Computer name, software, etc.)
- Is resident data potentially involved?
- What department/function is affected?
- Has anyone else reported this?
- What actions have you already taken?
- Your contact information (name, phone, email)

Don't worry about having all the answers - report what you know and we'll investigate.

6. IMMEDIATE ACTIONS - DO'S AND DON'TS

DO:

- Report the incident immediately using the contact information at the top of this guide
- Document what you observed (take photos of error messages if possible) • Preserve any evidence (don't delete emails or files)
- Disconnect from network if actively under attack (unplug network cable)
- Note the time you discovered the incident

- Keep the affected device powered on unless instructed otherwise
- Follow instructions from MCS Tech Services responders

DO NOT:

- Do not attempt to fix it yourself before reporting
- Do not shut down the computer (unless instructed by MCS TECH)
- Do not delete any files, emails, or logs
- Do not notify residents or media - this is handled by Town Supervisor
- Do not post about the incident on social media
- Do not discuss confidential details with unauthorized persons
- Do not wait to report because you're "not sure" - report it anyway
- Do not reboot servers without approval from MCS TECH

7. WHAT TO EXPECT - OUR RESPONSE PROCESS

When you report an incident to MCS Tech Services, here's what happens:

Phase 1: Initial Response (0-1 hour)

- We acknowledge your report and confirm receipt
- Security Operations Manager or on-call technician begins assessment
- We determine incident severity and scope
- You will receive initial instructions
- We notify appropriate town leadership based on severity

Phase 2: Containment (1-4 hours)

- We isolate affected systems to prevent spread
- We preserve evidence for investigation
- We implement temporary workarounds if possible
- We provide regular status updates
- Town Supervisor briefed if critical incident

Phase 3: Investigation & Recovery (Varies)

- We identify root cause and scope of incident
- We remove threats and restore systems
- We verify systems are clean and operational
- We document everything for compliance
- We provide recommendations to prevent recurrence

Phase 4: Post-Incident (1-2 weeks)

- We provide final incident report
- We conduct lessons-learned review

- We implement security improvements
- We update policies and procedures as needed

8. COMMUNICATION DURING INCIDENTS

Internal Communication:

During an incident, MCS Tech Services will keep you informed through:

- Regular status updates (frequency based on severity)
- Email updates to Town Supervisor and affected department heads
- Phone calls for critical updates • Final incident report when resolved

External Communication:

All external communications must be coordinated:

- Town Supervisor has final authority on external communications
- MCS TECH will provide technical information and recommendations
- Town Attorney should be consulted for legal requirements
- Town Clerk involved for FOIL and public records considerations
- No employee should speak to media without Town Supervisor approval

REMEMBER: Incident response communications may become public records under FOIL. Keep communications professional and factual.

9. MUNICIPAL GOVERNMENT CONSIDERATIONS

9.1 New York State Requirements

As a New York municipality, certain legal requirements apply to cybersecurity incidents:

- **Data Breach Notification (NY Gen. Municipal Law § 18):** If resident private information is breached (SSN, driver's license, account numbers with security codes), the town must notify affected residents, the NY Attorney General, and consumer reporting agencies. MCS TECH will help determine if this applies and assist with notification.
- **FOIL Considerations (NY Public Officers Law Article 6):** Incident response communications and records may be subject to FOIL requests. Documents will be created with this in mind. Never delete incident records.

- **Public Records Retention:** Incident documentation must be retained per NY State Archives retention schedules. MCS TECH will provide final documentation that must be filed with Town Clerk.
- **Town Board Notification:** Critical incidents requiring significant expenditures, legal action, or public notification should be reported to the Town Board. Town Supervisor determines timing and method.

9.2 Resident Notification

If an incident involves resident data, notification may be required:

- MCS TECH and Town Attorney will determine legal notification requirements
- Town Supervisor approves all resident notification language
- Notifications must be timely (typically within days of discovering breach)
- MCS TECH will provide technical details for notification letters.
- Consider offering credit monitoring if SSNs were exposed
- Document all notification efforts

9.3 Elected Officials and Staff

Incident response applies equally to elected officials and appointed staff:

- Town Board members must report incidents on their devices
- All email accounts (elected and staff) must be protected equally
- Personal devices used for town business are covered
- Elected officials' communications during incident may be FOIL-able
- Chain of command: Employee → Department Head → Town Supervisor → Town Board (if needed)

10. PREVENTING INCIDENTS

The best incident is one that never happens. Help protect the town by following security best practices:

- Use strong, unique passwords and never share them
- Enable multi-factor authentication on all accounts
- Be suspicious of unexpected emails, especially with attachments or links
- Keep systems updated - install updates promptly
- Lock your computer when stepping away (Windows+L)
- Don't click links or download attachments from unknown senders
- Report suspicious emails immediately - don't just delete them
- Use only approved software and applications
- Don't plug in unknown USB drives

- Be cautious on public WiFi - use VPN when working remotely
- Shred confidential documents before disposal
- Report lost or stolen devices immediately
- Complete required security awareness training
- If you are in doubt, ask - contact MCS TECH if you're unsure about something

11. AFTER-HOURS AND WEEKEND INCIDENTS

Cybersecurity incidents don't only happen during business hours. Attackers often target nights and weekends when response may be slower.

When to Call After Hours:

Call (845) 259-1700 immediately (24/7) if:

- **Systems are actively being encrypted (ransomware)**
- **Critical systems are down and affecting operations**
- **You discover a data breach involving resident information**
- **Emergency services systems are compromised**
- **Widespread system problems affecting multiple departments**
- **Any incident that cannot wait until Monday morning**

Lesser incidents can be reported via email and will be addressed first thing the next business day.

Holiday and Weekend Procedures:

- Emergency line is monitored 24/7/365 including holidays
- On-call technician will respond within 1 hour for emergencies
- Town Supervisor should be notified of any after-hours critical incidents
- Keep this guide accessible even when office is closed

12. TRAINING AND QUESTIONS

Security Awareness Training:

MCS Tech Services provides regular security awareness training for town employees. This training covers:

- Recognizing phishing and social engineering attacks
- Password security and multi-factor authentication
- Safe internet and email practices
- Incident recognition and reporting
- Data protection and handling
- Physical security awareness

Training Schedule: Annually

Questions and Support:

If you have questions about this guide or security in general:

- Non-Emergency Questions:
  Email: support@mcstechinc.com
  Phone: (845) 259-1700 - 9am-5pm, Monday to Friday
- Security Emergencies:
  24/7 Emergency Line: (845) 259-1700 (Outside Business Hours)
- Technical Support:
  MCS Tech Services provides support through:
- Ticketing system (NinjaRMM)
- Support email
- Emergency phone line

13. DOCUMENT INFORMATION

Document Owner	**MCS Tech Services**
Prepared For	Town of Gardiner
Version	1.0
Effective Date	December 1, 2025
Review Frequency	Annually or after significant incidents
Next Review Date	December 1, 2026
Distribution	All town employees, elected officials, department heads

Revision History:

Version	Date	Author	Changes
1.0	December 1, 2025	MCS Tech Services	Initial release

QUICK REFERENCE CARD

(Cut out and keep at your desk)

TOWN OF GARDINER CYBERSECURITY INCIDENT RESPONSE

EMERGENCY CONTACTS (24/7)
Emergency Line: (845) 259-1700
Support Email: support@mcstechinc.com
Security Ops Manager: Kevin C. – kevin@mcstechinc.com

WHEN TO CALL IMMEDIATELY:

- ✓ Ransomware attack
- ✓ Systems locked or encrypted
- ✓ Data breach discovered
- ✓ Critical systems down
- ✓ Lost device with town data
- ✓ Clicked phishing link

DO NOT:

- ✗ Wait to report
- ✗ Shut down systems
- ✗ Delete anything
- ✗ Try to fix it yourself first

TOWN OF GARDINER

P.O. Box 1, GARDINER, NEW YORK 12525-0001 (845) 255-9675 Fax: (845) 255-9146

Town Hall Offices - 2340 Route 44/55 Gardiner NY 12525

Marybeth Majestic ***Julia L. Hansen***
Supervisor ***Town Clerk***

CYBERSECURITY INCIDENT NOTIFICATION GUIDE

I have read, received, and understand the above policy regarding the Cybersecurity Incident Notification Guide for the Town of Gardiner.

_____ _____ _____
Employe signature Printed Name Date

_ _

(cut here)

Acknowledgment of Receipt of the Cybersecurity Incident Notification Guide for the Town of Gardiner.

I have read, received, and understand the above policy regarding the Code of Ethics Policy of the Town of Gardiner.

_____ _____ _____
Employee signature Printed Name Date